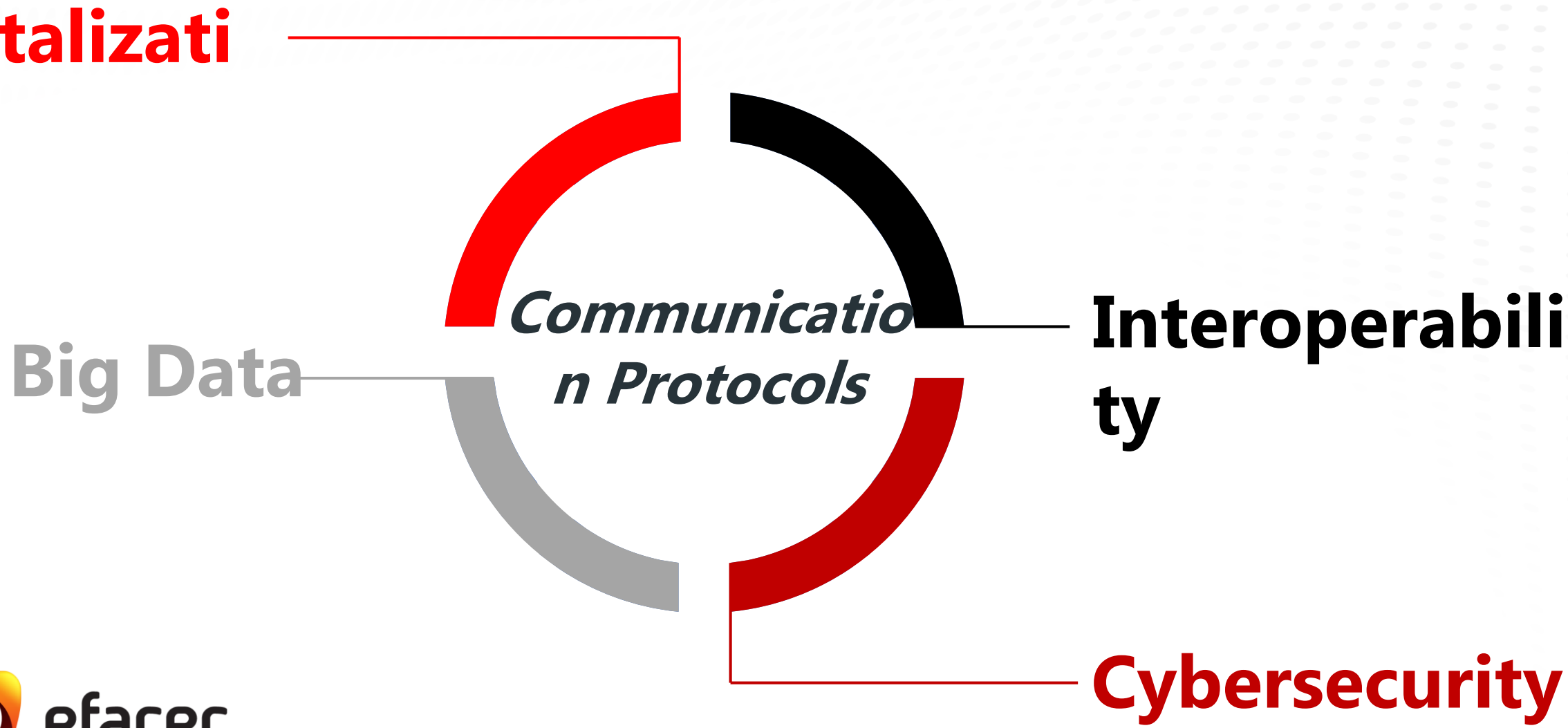
Moving Safely Towards IP Protocol for Signalling Equipment.

efacec Empowering the future

João Martins
Efacec
SW Development Leader

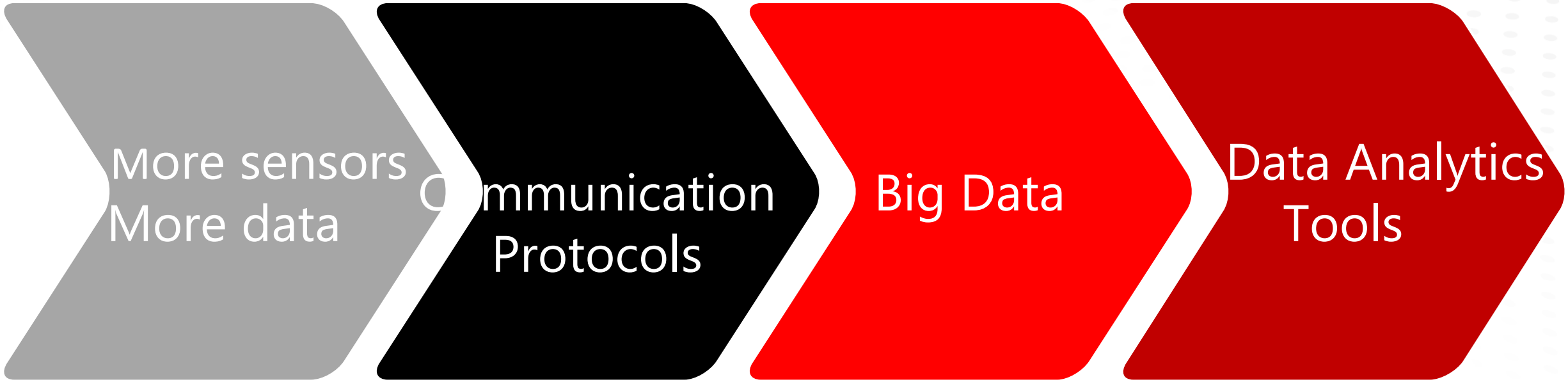
The Role of Communication Protocols



efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Digitalization

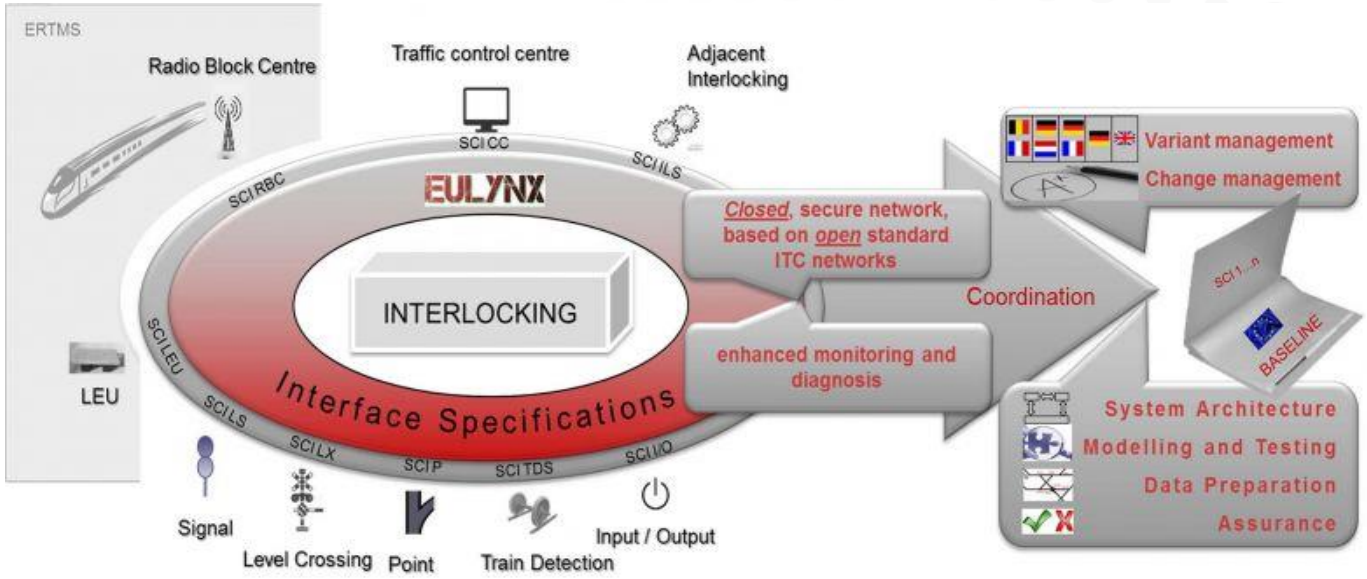


efacec

R&D Projects co-funded by:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Interoperability

- Accelerate systems evolution;
- Improve performance;
- Reduce development costs;
- Standardization;



efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Communication Protocols Challenges

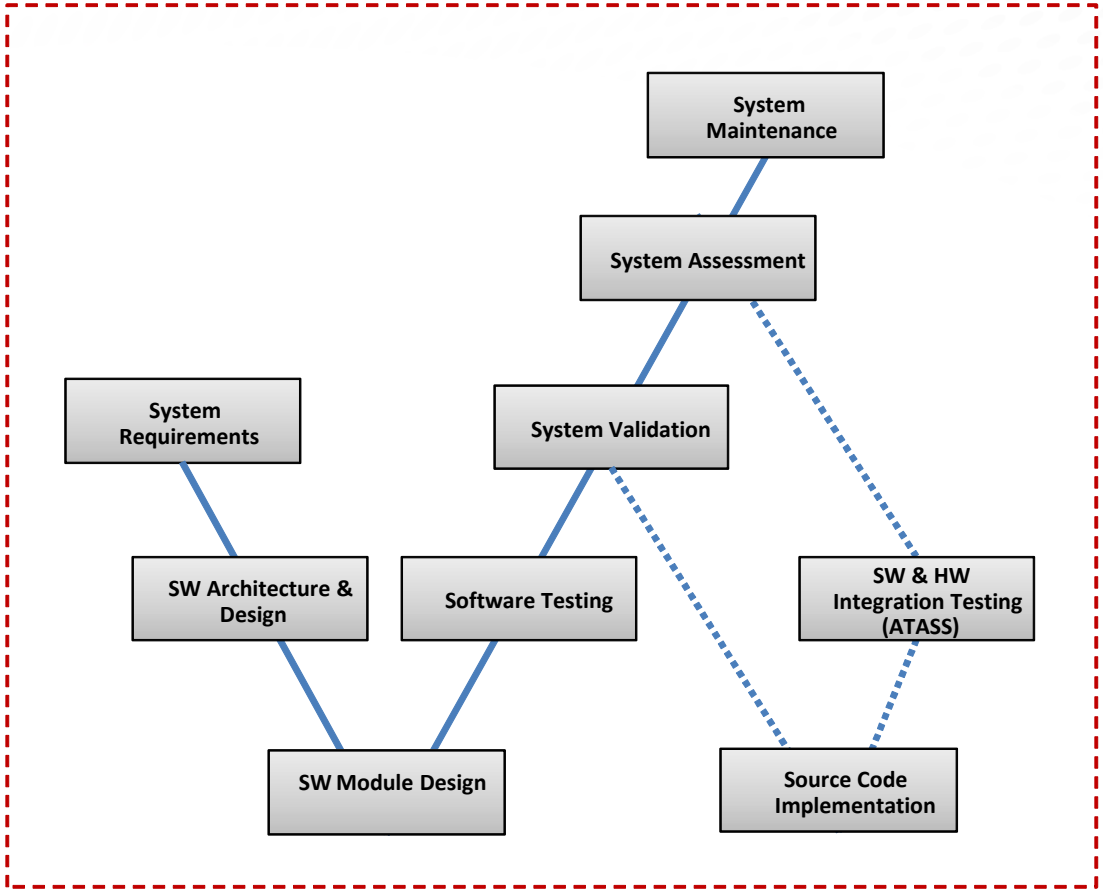
- Cybersecurity – ensure data authenticity;
- Safety – ensure data integrity;
- Railway standard for communications EN 50159;

An approach to implement safe communication protocols?

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

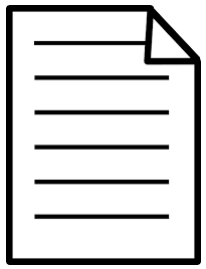
Development Process V-model



efacec

R&D Projects co-funded by:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Development Process Approach



Requirements Management

Architecture and Design

V&V

Source Code

Final Target System

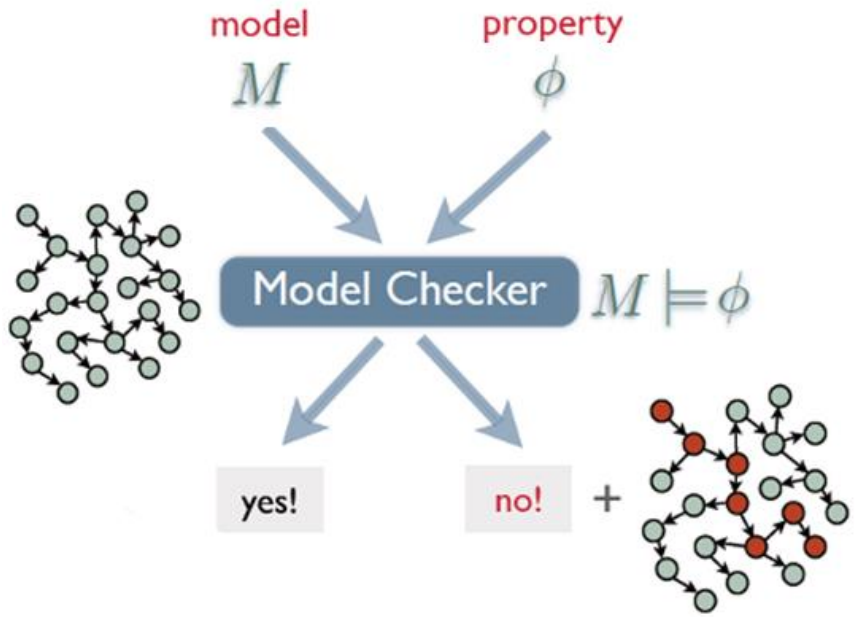
Final Target System Tests

efacec

R&D Projects co-funded by:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Formal Verification

- It is highly recommended for SIL 3/4 software systems (EN 50128);
- Apply formal verification at model level, using one of the most popular formal verification techniques: Model Checking;
- Define models and properties;
- Debug counter-examples;



efacec

R&D Projects co-funded by:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Properties Specification Approach

Threat	Defence Mechanism	Safety Properties
Delay	Timeout mechanism.	1) If no message is received within a given period of time then system shall enter in a fail state.
Repetition	Timestamp mechanism	2) If a message with timestamp not within the current timestamp and the timeout is received then it shall be discarded.
Insertion	Source identifiers	3) If a message from an unexpected source is received then it shall be discarded.
Insertion	Destination identifiers	4) If a message contains a destination identifier different from the expected one then the message shall be discarded.
Corruption	Safety code	5) If a message contains a safety code different than the one calculated then the message shall be discarded.

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Frauscher Safe Ethernet (FSE)

- A communication protocol to provide an interface between train detection system and higher-level signalling systems;
- Designed according railway standards for SIL 4 applications;
- FSE is a protocol certified according EN 50159 for Category 2;
- FSE is suitable for use in the majority of railway infrastructures;

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Modelling FSE

- The complete protocol was modelled with the exception of socket management function;
- Modelling challenges were overcome;
- The created model has successfully been integrated in a final target system;
- It is part of a solution working in a real scenario;

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Formal Verification of FSE

High-level Safety Properties	FSE Safety Properties
1) If no message is received within a given period of time then system shall enter in a fail state.	If no message is received within a given period of time then all statues shall be set with value 0.
3) If a message from an unexpected source identifier is received then it shall be discarded.	If the configured communication partner address does not match the source address of message then message shall be discarded.
4) If a message contains a destination identifier different from the expected identifier then the message shall be discarded.	If the receiver's own address and the destination address of the message does not match then message shall be discarded.
5) If a message contains a safety code different than the one calculated then the message shall be discarded.	If a received message contains a CRC code different than the one calculated then the message shall be discarded.
	If a received message contains a CRCi code different than the one calculated then the message shall be discarded.

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Conclusion

- The presented approach for the development of safe communication protocols has been validated by the successful implementation of FSE;
- The power of model-based process was proved once more;
- The key advantages of this approach are the efficiency provided by model-based development and the correctness obtained with formal verification process;
- The main challenges are the execution of formal verification due to the obstacles like state explosion and the modelling of safe protocols due to the expertise required;
- Understand the level of reuse provided by the property specification process;
- Contribution of this approach in the seek of weaknesses protocols design;

efacec

R&D Projects co-funded by:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Thank You!

efacec Empowering the future